UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/909,120	07/19/2001	John W.L. Ogilvie	1384.2.18A	1029

23484 7590 12/15/2004

JOHN W. L. OGILVIE
1320 EAST LAIRD AVENUE
SALT LAKE CITY, UT 84105

EXAMINER
WILLIAMS, JEFFERY L

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 12/15/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/909,120	**Applicant(s)** OGILVIE, JOHN W.L.	
	Examiner Williams Jeffery	**Art Unit** 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)□ Responsive to communication(s) filed on _____.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *7/19/01* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *07192001*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

Remarks

Claim Objections

Claims 8, 9, 10, 11, 12, and 13 are objected to because of the following informalities: They make reference to “the method of step…”. It is the Examiner’s belief that the Applicant means to say “the method of claim…”. Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 11, 12, and 13 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 1 – 5 are method claims which can be performed without computer implementation or the use of technology. Claims 6 – 13 are method claims directed toward use in software only, and are not tangibly embodied on or in some form of computer readable medium.

Notice

To expedite a complete examination of the instant application the claims rejected under 35 U.S.S. 101 (nonstatutory) above are further rejected as set forth below in anticipation of applicant amending these claims to place them within the four statutory categories of invention.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

Claims 1, 2, 3, 4, 5, 6, 14, 15, 16, are rejected under 35 U.S.C. 102(b) as being anticipated by Schneier, Applied Cryptography, 2nd Ed., 1997.

Regarding claim 1, Schneier anticipates the claimed invention by disclosing a method for enhancing the security of information, comprising the steps of:

Gathering at least two plaintext messages, each plaintext message containing information (Pg. 227, lines 23 - 27).

Creating an encrypted mux message from the at least two plaintext messages, such that the encrypted mux message comprises encryptions of the at least two plaintext messages (Pg. 227, lines 23 – 27).

The encrypted mux message has characteristics which disguise the encrypted mux message as an encryption of fewer plaintext messages than it actually contains (Pg. 227, lines 23 – 26; Pg. 228, lines 1, 2). The file is effectively "disguised" since one is not able to tell that the encrypted file contains a message other than the one obtained by supplying a given key.

Regarding claim 2, Schneier anticipates the claimed invention by disclosing:

The method of claim 1, wherein the creating step creates an encrypted mux message which has at least four of the following characteristics in common with an encryption of a single plaintext message: syntax, file name, file name extension, creation date, modification date, length, header, checksum, digital signature, storage directory (Pg. 226, lines 21 – 28; Pg. 227, lines 1,2; Pg. 228, lines 5 – 7). The teachings of Schneier disclose that encrypted files can be identified after making observation of the characteristics of the files, such a header or file format. He further discloses that for one to create an encrypted mux message, she may utilize an algorithm of her choice, generate ciphertext, and then store the resulting ciphertext on her hard disk. Thus, Schneier demonstrates the understanding that creating encrypted mux messages will produce files that will posses inherent characteristics in common with encryptions of regular messages, namely a syntax, a length, and a creation date, and possibly a header. Furthermore, since Schneier reveals that the created ciphertext may be placed on a hard drive, the encrypted file would also posses a storage directory.

Regarding claim 3, Schneier anticipates the claimed invention by disclosing:

The method of claim 1, wherein the creating step creates an encrypted mux message which has at least three of the following characteristics in common with an encryption of a single plaintext message: syntax, file name, file name extension, length, header, checksum, digital signature, storage directory (Pg. 226, lines 21 – 28; Pg. 227, lines 1,2; Pg. 228, lines 5 – 7). See claim 2 explanation above.

Regarding claim 4, Schneier anticipates the claimed invention by disclosing:

The method of claim 1, further comprising the step of choosing a plaintext message to be revealed (Pg. 227, lines 33 – 35).

The chosen plaintext message having an encryption in the encrypted mux message (Pg. 227, lines 33 – 36).

Regarding claim 5, Schneier anticipates the claimed invention by disclosing:

The method of claim 4, further comprising the step of making available to an unauthorized party a key for the chosen plaintext message, thereby permitting the unauthorized party to obtain the information in the chosen plaintext message by decrypting a portion of the encrypted mux message without permitting the unauthorized party to decrypt another portion of the encrypted mux message (Pg. 227, lines 27 – 37).

Regarding claim 6, Schneier anticipates the claimed invention by disclosing a method for use in a software program to enhance the security of information, comprising the steps of:

Accepting a key from a user (Pg. 227, lines 33 – 35).

Using the key to find a corresponding message encryption in a file containing encryptions of at least two plaintext messages (Pg. 227, lines 33 – 37).

The file being disguised to resemble a file containing fewer encryptions than are actually present in the file (Pg. 227, lines 23 – 26; Pg. 228, lines 1, 2). The “disguising” of the file is effectively accomplished since one is not able to tell that the encrypted file contains a message other than the one obtained by supplying a given key.

Decrypting the corresponding message encryption (Pg. 227, lines 35 – 37).

And making plaintext available to the user (Pg. 227, lines 35 – 37). Schneier discloses a method of encrypting a file. A decryption key is surrendered and applied to the file (the "acceptance" of the key). The result is a message corresponding to the particular key applied ("using the key to find a corresponding message", and "decrypting the corresponding message encryption").

Regarding claim 14, Schneier anticipates the claimed invention by disclosing:

An article comprising a computer-readable medium (Pg. 228, lines 7).

Configured with an embodied encrypted mux message (Pg. 227, lines 23 – 37).

That is disguised to hide at least one encryption (Pg. 228, lines 25 – 31).

And that is also susceptible of being at least partially decrypted in response to provision of a key corresponding to an encryption of plaintext within the encrypted mux message (Pg. 227, lines 23 – 28).

Regarding claim 15, Schneier anticipates the claimed invention by disclosing:

The article of claim 14, wherein the encrypted mux message is structured to contain contiguously stored message encryptions (Pg. 228, lines 18 – 20).

Regarding claim 16, Schneier anticipates the claimed invention by disclosing:

The article of claim 14, wherein the encrypted mux message is structured to contain interleaved stored message encryptions (Pg. 228, lines 12 –15).

Claims 6, 10, 11, 12, 14, 17, 18, 19, 20 are rejected under 35 U.S.C. 102(b) as being anticipated by Auerbach et al., Creation and Distribution of Cryptographic Envelope, US Patent: 5,673,316, Sep. 30, 1997.

Regarding claim 6, Auerbach et al. anticipates the claimed invention by disclosing a method for use in a software program to enhance the security of information, comprising the steps of:

Accepting a key from a user (Col. 12, lines 66,67; Col. 13, lines 1 - 5).

Using the key to find a corresponding message encryption in a file containing encryptions of at least two plaintext messages (Col. 12, lines 21 – 24).

The file being disguised to resemble a file containing fewer encryptions than are actually present in the file (Col. 3, lines 59 – 64). The "disguising" is accomplished by encoding the encrypted messages into an appropriate file format (i.e. zip., tar), thus obscuring the presence the individual messages encryptions.

Decrypting the corresponding message encryption (Col. 12, lines 34,35).

And making plaintext available to the user (Col.12, lines 35, 36).

Regarding claim 10, Auerbach et al. anticipates the claimed invention by disclosing:

The method of step 6, wherein the step of making plaintext available to the user comprises at least one of the following: displaying the plaintext on a computer screen, saving a copy of the plaintext in a file, transmitting a copy of the plaintext over a network (Col. 4, lines 9 – 12; Col. 6, lines 45 – 47; Col. 10, lines 62 – 64; Col. 7, lines 19 – 23). As taught by Auerbach et al., plaintext (i.e. books in digital form, JPEGs, or MPEG streams), may be encrypted and included as contents within a file containing other encryptions. The encrypted contents may be accessed by a user only if their corresponding decryption keys are provided to the DFWM module. The DFWM, in turn, decrypts the contents and provides the necessary watermarking. In reference to this watermarking, Auerbach et al., discloses the perusal of the watermarked documents, which by necessity implies that such documents (i.e. books in digital form, JPEGs, or MPEGs) are made available to the user in a form allowing for perusal (i.e. file or on screen display).

Regarding claim 11, Auerbach et al. anticipates the claimed invention by disclosing:

The method of step 6, wherein the step of making plaintext available to the user makes available the plaintext for the message encryption corresponding to the key provided (Col. 1, lines 45 – 48, 61 – 63; Col. 2, lines 20 – 22, 36 – 41). As taught by Auerbach et al., the informational contents encrypted with their corresponding keys are protected from disclosure until, upon purchase by a user, they are decrypted with their corresponding key, and their plaintext is made available to the user.

Regarding claim 12, Auerbach et al. anticipates the claimed invention by disclosing:

The method of step 6, wherein the step of making plaintext available to the user makes available a watermarked version of the plaintext for the message encryption corresponding to the key provided (Col. 10, lines 62 – 67).

Regarding claim 14, Auerbach et al. anticipates the claimed invention by disclosing:

An article comprising a computer-readable medium (Fig. 1, elem. 101).

Configured with an embodied encrypted mux message (Fig. 1, elem. 101; step 2).

That is disguised to hide at least one encryption (Col. 3, lines 59 – 64).

And that is also susceptible of being at least partially decrypted in response to provision of a key corresponding to an encryption of plaintext within the encrypted mux message (Col. 2, lines 36 – 41).

As taught by Auerbach et al., the cryptographic envelope, or "encrypted mux message", is created by a Document Server [100] and transmitted [step 2] to a User PC [101], of which would inherently posses a medium that would be configured with the cryptographic envelope upon receiving the transmitted cryptographic envelope. Also, as explained in connection with claim 1, the "disguising" of the cryptographic envelope is accomplished by encoding the encrypted messages into an appropriate file format (i.e. zip., tar), thus obscuring the presence the individual messages encryptions.

Regarding claim 17, Auerbach et al. anticipates the claimed invention by disclosing:

The article of claim 14, wherein the encrypted mux message contains message selection hints (Col. 4, lines 13 – 18). Auerbach et al. discloses the use of 'teasers' and plaintext abstracts within his cryptographic envelopes. Such teasers and abstracts would give the user a general idea, or "hint", of the actual content of particular encrypted portions of the envelope. Thus, the user is helped to select the encrypted portion he would like to have in clear text.

Regarding claim 18, Auerbach et al. anticipates the claimed invention by disclosing:

A computer system comprising a storage medium (Fig. 1, elems. 100 – 103).

Configured by an encrypted mux message stored therein (Fig. 1, elem. 101; step 2).

And a software security enhancing means for enhancing the security of information by using the encrypted mux message (Fig. 1, elems. 100 – 103). As taught by Auerbach et al., the cryptographic envelope, or "encrypted mux message", is created by a Document Server [100] and transmitted [step 2] to a User PC [101], of which would inherently posses a medium that would be configured with the cryptographic envelope upon receiving the transmitted cryptographic envelope. Further disclosed by Auerbach et al., the DFWM [103], a portion of the software security enhancing means used to enable cryptographic envelopes, is also present on the user's PC.

Regarding claim 19, Auerbach et al. anticipates the claimed invention by disclosing:

The system of claim 18, wherein the security enhancing means comprises software for creating an encrypted mux message from at least two plaintext messages (Fig. 1, elem. 100; Col. 5, lines 51, 52).

Regarding claim 20, Auerbach et al. anticipates the claimed invention by disclosing:

The system of claim 18, wherein the security enhancing means comprises software for accepting a key from a user (Col. 8, lines 7 – 14; Col. 3, lines 1, 2).

Using the key to find a corresponding message encryption in the encrypted mux message (Col. 10, lines 58 – 64).

Decrypting the corresponding message encryption (Col. 10, lines 62 – 64).

And making plaintext available to the user (Col. 11, lines 3, 4). As disclosed by Auerbach et al., the user provides the appropriate decryption keys to the system via the generation of a buy request message. The Decryption Fingerprinting and Watermarking Module (DFWM) decrypts the encrypted documents with their corresponding keys. Since multiple keys and their corresponding encrypted documents can be provided to the DFWM, it is inherent that the DFWM utilizes the key corresponding to the appropriate encrypted document. Thus, implied is the fact that the software system uses the key to find the corresponding message encryption.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Pare, Jr. et al.

Schneier discloses a method for creating an encrypted file that contains the decryptions of two messages, each message decrypted by use of a different key. One message and corresponding key may be real, and the other message and key may be a decoy. Thus, in cases of coercion or duress, the decoy key may be supplied and the decoy message may be revealed (Pg. 227, lines 23 – 26). The concept is to keep confidential information secure from unauthorized access. Schneier differs from the claimed invention because he does not show the sending of a silent alarm when a particular key, such a decoy key, is used.

Pare, Jr. et al. discloses a system and method wherein a buyer can provide an authentic PIN and biometric sample so as to generate a "commercial transaction message" and thereby gain access to a secure system (Abstract, lines 4 – 7). Furthermore, under duress or coercion, the buyer may instead provide a decoy "emergency" PIN that will send a silent alarm (Col. 5, lines 19 – 23). In such a circumstance, the coercer is presented with false information even though the transaction appears to have completed successfully (Col. 5, lines 23 – 31). The concept is to keep confidential information secure from unauthorized access. Pare, Jr. et al. is evidence that those who desire to keep confidential information secure from unauthorized access would recognize the benefits of using a decoy key/PIN under conditions of coercion/duress which would, in turn, cause a silent alarm to be sent.

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include with the method of Schneier the step of sending a silent alarm when a decoy key is used, so as to keep confidential information secure from unauthorized access, as per the teachings of Pare, Jr. et al.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

R. Canetti, C. Dwork, M. Naor, and R. Ostrovsky. Deniable Encryption. "Lecture Notes in Computer Science." Volume 1294, pages 90-104. 1997. This article discloses a method for combining multiple messages into a single ciphertext that may be decrypted with keys corresponding the messages it contains.

G. Samid. Tailored Key Encryption (TaKE) Tailoring a key for a given pair of plaintext/ciphertext. Cryptology ePrint Archive, Report 2000/011. 2000. This article discloses a method for generating ciphertext that contains the decryptions of multiple messages.

Please direct all inquiries concerning this communication to Jeffery Williams, (571) 272-7965. The examiner can be normally reached Monday – Friday from 9am to 5pm, EST.

If attempts to reach examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell, can be reached at (571) 272-3868. The fax phone number for this group is (703) 305-3230.

Any inquiry of general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (571) 272-3795.

Andrew Caldwell
Andrew Caldwell